CLAIMS

1. (Original) Method for managing the security of applications with a security module functioning in an equipment connected to a network, said network being managed by a control server of an operator, said applications using resources as data or functions stored in a security module locally connected to said equipment, comprising the following preliminary steps:

- reception of data comprising at least the type and software version of the equipment and the identity of the security module, via the network, by the control server,

- analysis and verification by the control server of said data,

- generation of a cryptogram from the result of the verification of said data, and transmission of said cryptogram, via the network and the equipment, to the security module,

said method further comprises steps wherein the security module analyses the received cryptogram and activates, respectively deactivates the resources as data or functions used by at least one application installed in the equipment, said cryptogram comprising the instructions conditioning the functioning of the application according to criteria established by the supplier of said application and/or the operator and/or the user of the equipment.

2. (Original) Method according to claim 1, characterized in that the equipment is a mobile equipment of mobile telephony.

3. (Original) Method according to claim 1, characterized in that the network is a mobile network of the GSM, GPRS or UMTS type.

4. (Original) Method according to claims 1 and 2, characterized in that the security module is a subscriber module of a SIM card type inserted into the mobile equipment of mobile telephony.

5. (Original) Method according to claims 1 to 4, characterized in that the identification of the set mobile equipment / subscriber module is carried out from the identifier of the mobile equipment and from the identification number of the subscriber module pertaining to a subscriber to the mobile network.

6. (Original) Method according to claims 1 to 5, characterized in that the criteria defines the usage limits of an application according to the risk associated to said application and to the type and the software version of the mobile equipment that the operator and/or the application supplier and/or the user of the mobile equipment want to take in account.

7. (Original) Method according to claims 1 to 6, characterized in that it is carried out after each connection of the mobile equipment to the network.

8. (Original) Method according to claims 1 to 6, characterized in that it is carried out after each of updating the software version of the mobile equipment.

9. (Original) Method according to claims 1 to 6, characterized in that it is carried out after each activation or deactivation of an application on the mobile equipment

10. (Original) Method according to claims 1 to 6, characterized in that it is carried out after each updating of the software version of the subscriber module.

11. (Original) Method according to claims 1 to 6, characterized in that it is carried out after each updating of the resources on the subscriber module.

12. (Original) Method according to claims 1 to 6, carried out periodically at a rate given by the control server.

13. (Original) Method according to claims 1 to 6, characterized in that it is carried out after each initialization of an application on the mobile equipment.

14. (Original) Method according to any of the preceding claims, characterized in that the subscriber module, prior to the execution of the instructions given by

the cryptogram, compares the identifier of the mobile equipment with that previously received and only initiates the verification operation if the identifier has changed.

15. (Original) Method according to claims 1 to 5, characterized in that the control server, prior to the transmission of the cryptogram, compares the identifier of the mobile equipment with that previously received and only initiates the verification operation if the identifier has changed.

16. (Original) Method according to claims 1 to 15, characterized in that the cryptogram is made up of a message encrypted by the control server with the aid of an asymmetrical or symmetrical encryption key from a data set containing, among other data, the identifier of the mobile equipment, the identification number of the subscriber module, the resource references of the subscriber module and a predictable variable.

17. (Original) Method according to claims 1 to 16 characterized in that the subscriber module transmits to the control server, via the mobile equipment and the mobile network, a confirmation message when the subscriber module has received the cryptogram, said message confirming the correct reception and the adequate processing of the cryptogram by the subscriber module.

18. (Original) Method according to claim 1, characterized in that characterized in that the equipment is a Pay-TV decoder or a computer to which the security module is connected.

19. (Original) Security module comprising resources intended to be locally accessed by at least one application installed in an equipment connected to a network, said equipment comprising reading and data transmission means comprising at least the identifier of the equipment and the identifier of the security module, said module further comprises means for reception, analysis and execution of instructions contained in a cryptogram, said instructions conditioning

the functioning of the application according to criteria predetermined by the supplier of said application and/or the operator and/or the user of the equipment.

20. (Original) Security module according to claim 19, characterized in that it constitutes a subscriber module of the "SIM card" type connected to a mobile equipment.